Amendments to the Claims:

1. (currently amended) A method for delivering information from a trust information provider to a client having memory for verification of a received certificate by said client, comprising the steps of:

downloading ~~providing~~ a trust information object (TIO) from a server to said memory of said client, ~~wherein for each of a plurality of trust entity certificates~~ said TIO comprising at least a plurality of ~~es: 1) a~~ hash values, each hash value being hashed from a trusted entity certificate, and a plurality of trust vectors, each trust vector corresponding to a hash value and being indicative of the level of trust associated with a particular trusted entity certificate ~~of said trust entity certificate, and 2) associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate, wherein the trusted entity comprises a certificate authority~~; and

verifying a received certificate by hashing said received certificate to generate a resulting hash value, comparing said resulting hash value to said hash values in said TIO to determine if a match exists, and, if said match is found, determining if the corresponding trust vector indicates requisite level of trust to establish connection ~~using at least a portion of said TIO~~.

2. (currently amended) The method of Claim 1, wherein said TIO further comprises:

~~for each of said trust entity certificates, a trust vector including at least a portion of said trust information;~~

a value indicating a number of signatures required for a next update;

a timestamp of when ~~date~~ said TIO is created; and

a digital signature of all data including said trust entity certificates, said trust vectors, said number of signatures, and said timestamp included in said TIO.

3. (previously presented) The method of Claim 1, wherein said hash values are determined using any of MD5 and SHA-1.

4. (previously presented) The method of Claim 1, wherein said TIO conforms to the PKCS#7 standard.

5. (previously presented) The method of Claim 1, further comprising the steps of: hard coding said TIO into said client's software.

6. (original) The method of Claim 1, further comprising the step of:
saving a copy of said TIO in a persistent memory during said client's build time.

7. (withdrawn) A method for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising the steps of:

associating a trust information object (TIO) with said client, said TIO comprising a hash value of a trust entity certificate and associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate;

during an SSL handshake between said client and said server, said server sending a certificate chain that, optionally, contains a root certificate (RC) to said client; and

said client validating said server certificate using said TIO.

8. (withdrawn) The method of Claim 7, wherein said client hashes a server certificate and compares a resulting digest against a list of trusted entity certificate thumbprints obtained from said TIO.

9. (withdrawn) The method of Claim 8, wherein if a thumbprint match is not found:

said client retrieves an RC from a trusted server;

said client performs certificate chain validation up to a root certificate authority (CA);

once an entire certificate chain is validated, said client tries to validate said CA RC;

wherein, if said RC is included in said certificate chain, said client hashes said RC and looks up said TIO in said client;

wherein if a resulting hash value and a corresponding trust bit are found in said TIO, then said certificate chain is considered to be valid and session initiation proceeds.

10. (withdrawn) The method of Claim 8, wherein if a thumbprint match is, said client checks a trust bit vector associated with said certificate to ensure that an authenticated server is trusted in the context of a session being established.

11. (withdrawn) The method of Claim 9, wherein if necessary trust capabilities are not set on a matched thumbprint, said client fails a session initiation handshake.

12. (withdrawn) The method of Claim 7, wherein a hash value in said TIO is taken by hashing a valid certificate; and wherein said certificate is accepted by a validation mechanism, even when said client receives an expired root certificate.

13. (withdrawn) The method of Claim 7, further comprising the step of:

providing in said TIO a designated trust bit associated with a site certificate for identifying a site that is trusted to perform certain operations;

wherein when said client executes a script it checks said certificate and associated trust information; and

wherein if said trust bit indicates that a site identified by its certificate is trusted for an intended operation, then access permission is granted.

14. (currently amended) A method for delivering information from a server to a client having memory, comprising the steps of:

downloading a trust information object (TIO) from said server to said memory of said client, said TIO comprising at least a plurality of hash values, each hash value being hashed from a trusted entity certificate, and a plurality of trust vectors, each trust vector corresponding to a hash value and being indicative of the level of trust associated with a particular trusted entity certificate; and

~~embedding a trust information object (TIO) within said client, wherein for each of a plurality of trust entity certificates said TIO comprises: 1) a hash value of said trust entity certificate, and 2) associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate, wherein said trusted entity comprises a certificate authority;~~

said client periodically connecting to said server to determine whether a new TIO is available; and

said server sending a new TIO to said client if said new TIO is available.

15. (currently amended) The method of Claim 14, further comprising the step of: sending ~~a~~said TIO with ~~including~~ a signing certificate to said client, wherein trust information of said signing certificate indicates that said certificate can be trusted for signing said TIO.

16. (previously presented) The method of Claim 15, wherein said client fetches said TIO from a trusted server, said client ensuring that a root certificate that signed said signing certificate is contained in said TIO and is not revocable.

17. (previously presented) The method of Claim 14, wherein said client verifies a digital signature of said TIO with a signing certificate, along with a TIO sent to said client.

18. (original) The method of Claim 17, wherein multiple signatures are verified, depending on the number of signatures specified in said TIO; wherein said client

hashes said signing certificates one by one; and wherein if proper results are found in said TIO and said certificates are trusted for signing said TIO, then said TIO proves that it was not tampered with.

19. (original) The method of Claim 18, wherein said signing certificates exist in said TIO in said client before said TIO is signed.

20. (previously presented) The method of Claim 14, wherein said TIO is delivered to said client via a broadcast channel; wherein a provider delivers a TIO to said client that contains a signing certificate and associated trust information by either of including said signing certificate in an initial TIO saved in a client persistent memory, or by sending said TIO to said client through a secure channel before using said broadcast channel.

21. (original) The method of claim 14, further comprising the step of: updating said TIO on a per session basis when said TIO is not persistently stored.

22. (currently amended) An apparatus for receiving information from a server for verification of a received certificate, comprising:

a client device ~~for receiving a trust information object (TIO) associated with said client device, said client device~~ comprising a memory having resident therein a trust information object (TIO) downloaded from ~~for storing said TIO,~~ from a server to said memory, said TIO comprising at least a plurality of hash values, each hash value being hashed from a trusted entity certificate, and a plurality of trust vectors, each trust vector corresponding to a hash value and being indicative of the level of trust associated with a particular trusted entity certificate; and

~~wherein for each of a plurality of trust entity certificates said TIO comprises: 1) a hash value of said trust entity certificate; and 2) associated trust information indicating a level of trust for a trusted entity associated with~~

~~said trust entity certificate, wherein said trusted entity comprises a certificate authority~~;

wherein said client device is adapted for verifying a received certificate by hashing said received certificate to generate a resulting hash value, comparing said resulting hash value to said hash values in said TIO to determine if a match exists, and, if said match is found, determining if the corresponding trust vector indicates requisite level of trust to establish connection ~~using at least a portion of said TIO.~~

23. (cancelled)

24. (currently amended) The apparatus of Claim 22, wherein said TIO further comprises at least one of:

~~for each of said trust entity certificates, a trust vector including at least a portion of said trust information;~~

a value indicating a number of signatures required for a next update;

a time stamp which indicates a date that said TIO is generated; and

for each of said trust entity certificates, a thumb print comprising a hash of a public key embedded in said certificate that represents said trusted entity.

25–28. (cancelled)

29. (currently amended) The apparatus of Claim ~~25~~22, wherein said TIO comprises a TIO derived from a set of root certificate authority (CA) certificates hard coded into software of said client device.

30. (currently amended) The apparatus of Claim ~~25~~22, wherein said TIO further comprises:

a copy of said TIO saved in a persistent memory during said client's build time.

31. (withdrawn) An apparatus for delivering certificates with associated trust information from a server to a client for verification of a received certificate by said client, comprising:

a trust information object (TIO) associated with said client, said TIO comprising a hash value of a trust entity certificate and associated trust information indicating a level of trust for a trusted entity associated with said trust entity certificate;

means for sending a certificate chain from said server that, optionally, contains a root certificate (RC) to said client during an SSL handshake between said client and said server; and

means at said client for validating said server certificate using said TIO.

32. (withdrawn) The apparatus of Claim 31, wherein said client hashes a server certificate and compares a resulting digest against a list of trusted entity certificate thumbprints obtained from said TIO.

33. (withdrawn) The apparatus of Claim 32, wherein if a thumbprint match is not found:

said client retrieves an RC from a trusted server;

said client performs certificate chain validation up to a root certificate authority (CA);

once an entire certificate chain is validated, said client tries to validate said CA RC;

wherein, if said RC is included in said certificate chain, said client hashes said RC and looks up said TIO in said client;

wherein if a resulting hash value and a corresponding trust bit are found in said TIO, then said certificate chain is considered to be valid and session initiation proceeds.

34. (withdrawn) The apparatus of Claim 32, wherein if a thumbprint match is, said client checks a trust bit vector associated with said certificate to ensure that an authenticated server is trusted in the context of a session being established.

35. (withdrawn) The apparatus of Claim 34, wherein if necessary trust capabilities are not set on a matched thumbprint, said client fails a session initiation handshake.

36. (withdrawn) The apparatus of Claim 31, wherein a hash value in said TIO is taken by hashing a valid certificate; and wherein said certificate is accepted by a validation mechanism, even when said client receives an expired root certificate.

37. (withdrawn) The apparatus of Claim 31, further comprising:

a designated trust bit in said TIO associated with a site certificate for identifying a site that is trusted to perform certain operations;

wherein when said client executes a script it checks said certificate and associated trust information; and

wherein if said trust bit indicates that a site identified by its certificate is trusted for an intended operation, then access permission is granted.

38–49. (cancelled)

50. (new) The method of claim 1, wherein said TIO is updated periodically by said TIO-provider server.

51. (new) The method of claim 1, wherein downloading said TIO comprises broadcasting said TIO.

52. (new) The method of claim 51, wherein said TIO is signed.

52. (new) The method of claim 1, wherein said TIO is downloaded each time a received certificate is verified.

53. (new) The method of claim 52, wherein said TIO is cached in memory.

54. (new) The method of claim 1, wherein said TIO is stored in persistent memory.

55. (new) The method of claim 54, wherein TIO is downloaded using one of broadcast or http.